

EXHIBIT B

(12) **EX PARTE REEXAMINATION CERTIFICATE** (9079th)
United States Patent
Feldbau et al. (10) **Number:** **US 6,182,219 C1**
(45) **Certificate Issued:** **Jun. 19, 2012**

(54) **APPARATUS AND METHOD FOR AUTHENTICATING THE DISPATCH AND CONTENTS OF DOCUMENTS**

(75) Inventors: **Ofra Feldbau**, Ramat Gan (IL); **Michael Feldbau**, Ramat Gan (IL)

(73) Assignee: **Rmail Limited**, Pembroke (BM)

Reexamination Request:

No. 90/011,580, Mar. 17, 2011

Reexamination Certificate for:

Patent No.: **6,182,219**
Issued: **Jan. 30, 2001**
Appl. No.: **08/981,461**
Filed: **Dec. 23, 1997**

Certificate of Correction issued Dec. 24, 2002.

(22) PCT Filed: **Aug. 27, 1996**

(86) PCT No.: **PCT/IB96/00859**

§ 371 (c)(1),
(2), (4) Date: **Dec. 23, 1997**

(87) PCT Pub. No.: **WO97/08869**

PCT Pub. Date: **Mar. 6, 1997**

(30) **Foreign Application Priority Data**

Aug. 28, 1995 (EP) 95113489
Feb. 22, 1996 (IL) 117234

(51) **Int. Cl.**
H04L 9/32 (2006.01)

(52) **U.S. Cl.** **713/176; 713/178; 713/170;**
713/155; 705/75; 380/258; 380/259; 380/260

(58) **Field of Classification Search** **713/176**
See application file for complete search history.

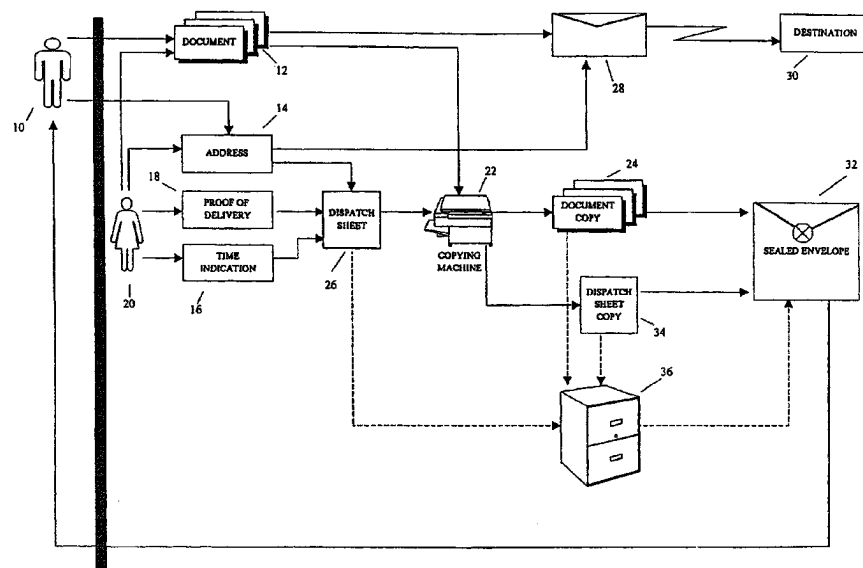
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/011,580, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner—Andrew Nalven

(57) **ABSTRACT**

Apparatus and method for authenticating that a sender has sent certain information via a dispatcher to a recipient is disclosed. The method includes the steps of: (a) providing a set A comprising a plurality of information elements a1, . . . an, said information element a1 comprising the contents of said dispatched information, and said one or more information elements a2, . . . an comprising dispatch-related information and comprise at least the following elements: a2—a time indication associated with said dispatch; and a3—information describing the destination of said dispatch, and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender, (b) associating said dispatch-related information with said element a1 by generating authentication-information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; (c) securing at least part of said authentication-information against undetected tamper attempts of at least said sender. The dispatch relates either to transmission or to manual delivery. The apparatus implements the operations of the method.



US 6,182,219 C1

1
EX PARTE
REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS
INDICATED BELOW.

Matter enclosed in heavy brackets [] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN
DETERMINED THAT:

Claims 1, 2, 30, 39, 60, 65, 66, 71, 77, 78, 82, 85 and 86 are determined to be patentable as amended.

Claims 3-29, 31-38, 40-59, 61-64, 67-70, 72-76, 79-81, 83, 84 and 87-89 dependent on an amended claim, are determined to be patentable.

1. Apparatus for authenticating that certain information has been *successfully* transmitted from a sender via a dispatcher to a recipient, the apparatus comprising:

means for providing a set A comprising a plurality of information a1, . . . , an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2, . . . , an comprising dispatch-related information and comprise at least the following elements:

a2—[a time indication associated with said dispatch] *an indicia of a time of the successful transmission of the certain information to the recipient, the indicia recorded by the dispatcher*; and

a3—information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the receiver and having

(1) means for associating said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

(2) means for securing at least part of said authentication-information against tampering of said sender and recipient;

wherein at least one of the means for associating and for securing comprises means for generating a new set B, said set B comprising one or more information elements b1, . . . , bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.

2

2. Apparatus according to claim 1, wherein said element a2 comprises at least one element selected from the group consisting of [the] a date associated with said [dispatch] *successful transmission of the certain information to the recipient*, and [the] a time associated with said [dispatch] *successful transmission of the certain information to the recipient*.

30. A method for authenticating that certain information has been *successfully* transmitted from a sender via a dispatcher to a recipient, comprising the steps of:

providing a set A comprising a plurality of information elements a1, . . . , an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2, . . . , an comprising dispatch-related information and comprise at least the following elements:

a2—[a time indication associated with said dispatch] *an indicia of a time of the successful transmission of the certain information to the recipient, the indicia recorded by the dispatcher*; and

a3—information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient;

associating, by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

securing, by said authenticator, at least part of said authentication-information against tampering of said sender and recipient;

wherein at least one of the steps of associating and securing comprises the step of generating a new set B, said set B comprising one or more information elements b1, . . . , bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said A functions Fi can be different.

39. A method according to claim 30, wherein said element a2 comprises at least one element selected from the group consisting of [the] a date associated with said [dispatch] *successful transmission of the certain information to the recipient*, and [the] a time associated with said [dispatch] *successful transmission of the certain information to the recipient*.

60. A method of authenticating a dispatch and contents of the dispatch *successfully* transmitted from a sender to a recipient, comprising the steps of:

receiving content data representative of the contents of the dispatch originated from the sender and being electrically transmitted to said recipient, and a destination of the dispatch;

providing an indicia [relating to] of a time of *successful* transmission of the dispatch *to the recipient*, said time related indicia being *recorded by an authenticator and* provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

US 6,182,219 C1

3

associating, by [an] *the* authenticator functioning as a non-interested third party with respect to the sender and the recipient, the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and
 securing, by said authenticator, at least part of the authentication data against tampering of the sender and the recipient;
 wherein at least one of the steps of associating and securing utilizes mathematical association methods for a selected portion of a combination of the content data and the dispatched record data.

65. A method according to claim 60, wherein the step of providing the time [related] indicia includes receiving the time [related] indicia from an external source.

66. A method according to claim 60, wherein the step of providing the time [related] indicia includes generating the time [related] indicia.

71. An authenticator for authenticating a dispatch and contents of the dispatch *successfully* transmitted by or for a sender-from a transmitting system to a receiving system for a recipient via an electronic communication network, comprising:

an input unit coupled to the communication network or to the transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said receiving system, and a destination of the dispatch;

means for providing an indicia [relating to] *of a time of successful transmission of the dispatch to the receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;*

a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch to generate authentication data which authenticate the dispatch and the contents of the dispatch

means for securing at least part of the authentication data against tampering of the sender and the recipient, the authenticator functioning as a non-interested third party with respect to the sender and the recipient;

wherein the processor utilizes mathematical association methods for a selected portion of a combination of the content data and the dispatch record data to generate the authentication data.

77. An authenticator according to claim 71, wherein the means for providing the time [related] indicia receives the time [related] indicia from an external source.

4

78. An authenticator according to claim 71, wherein the means for providing the time [related] indicia generates the time [related] indicia.

82. An information dispatch system in an electronic communication network comprising;

a source transmitting system coupled to the electronic communicating network for sending a dispatch from a sender to a recipient;

a destination receiving system coupled to the electronic communication network for receiving the dispatch for the recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the recipient for authenticating the dispatch and contents of the dispatch transmitted from the source transmitting system to the destination receiving system, including:

(1) an input unit coupled to the communication network or to the source transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said destination receiving system, and a destination of the dispatch;

(2) means for providing an indicia [relating to] *of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;*

(3) a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

(4) means for securing at least part of the authentication data against tampering of the sender and the recipient;
 wherein the processor is combined with the means for securing.

85. An information dispatch system according to claim 82, wherein the means for providing the time [related] indicia receives the time [related] indicia from an external source.

86. An information dispatch system according to claim 82, wherein the means for providing the time [related] indicia generates the time [related] indicia.

* * * * *